公益社団法人医療系大学間共用試験実施評価機構

情報セキュリティ規程

Ver.0.10

2024年10月

共用試験制度・システム開発委員会 制作

令和７年４月１日から施行

更新履歴

更新日	版	主要更新内容
2024 年 10 月 20 日	0.10	新規作成

目　次

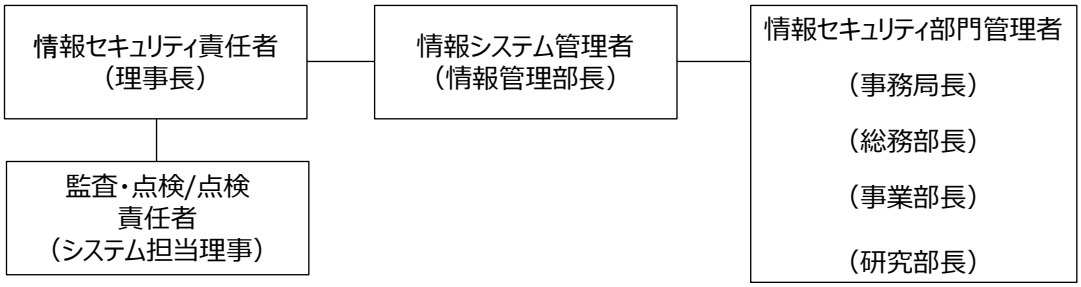
1. 組織としての対策（適用範囲：全機構職員，全機構委員）

1.1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として，情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし，情報セキュリティ対策状況の把握，情報セキュリティ対策に関する指針の策定・見直し，情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会の組織体制

役職名	役割，責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに，全責任を負う。
情報システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。 情報セキュリティ対策を推進するために従業員への教育を企画・実施する。 事故が発生した場合にはその影響を判断し，対応について意思決定する。
情報セキュリティ部門管理者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し，助言を行う。



1.2. 情報セキュリティ取組みの監査・点検/点検

監査・点検/点検責任者は，情報セキュリティ関連規程の実施状況について，毎年点検を行い，監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は，報告に基づき，以下の点を考慮し，必要に応じて改善計画を立案する。

- 情報セキュリティ関連規程が有効に実施されていない場合は，その原因の特定と改善
- 情報セキュリティ関連規程に定められたルールが，対策として不十分または有効でない場合は，情報セキュリティ関連規程の改訂
- 情報セキュリティ関連規程に定められたルールが，関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は，情報セキュリティ関連規程の改訂

1.3. 情報セキュリティに関する情報共有

情報システム管理者は，新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し，委員会で共有する。

2. 人的対策（適用範囲：全職員（常勤職員，非常勤職員，派遣職員を含む））

2.1. 雇用条件

職員を雇用する際には秘密保持契約を締結する。

2.2. 職員の範囲

職員は，常勤役員，常勤職員，派遣職員（以下，職員等とする。），および非常勤役員，各種委員会委員（以下，機構委員とする。）とする。

2.3. 職員の責務

職員は，以下を遵守する。

- 職員は，機構が業務秘密として管理する情報及びその複製物の一切を許可されていない組織，人に提供してはならない。
- 職員は，機構の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒については，就業規則に準じる。

※ 機構が業務秘密として管理する情報とは，「3.1.1 情報資産の特定と機密性の評価 」に示す「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

2.4. 雇用の終了

職員は，在職中に交付された業務に関連する資料，個人情報，顧客・取引先から当機構が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。

2.5. 機構委員の委嘱

会員大学の教員等を機構委員として委嘱する際には秘密保持契約を締結する。

2.6. 機構委員の責務

機構委員は以下を遵守する。

- 機構委員は，機構が業務秘密として管理する情報及びその複製物の一切を許可されていない組織，人に提供してはならない。
- 機構委員は，機構の情報セキュリティ方針及び関連規程を遵守する。

2.7. 任期の終了

機構委員は，任期中に交付された業務に関連する資料，個人情報，顧客・取引先から当機構が交付を受けた資料又はそれらの複製物，および業務中に知り得た情報の機構外への拡散を一切禁止する。

2.8. 情報セキュリティ教育

情報システム管理者は，全職員および全機構委員を対象として，情報セキュリティに関する教育計画を年度単位で立案する。

3. 情報資産管理（適用範囲：全機構職員，全機構委員）

3.1. 情報資産の管理

3.1.1. 情報資産の特定と機密性の評価

当機構の事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し，「情報資産管理台帳」に記載する。情報資産の機密性は，以下の基準に従って評価する。

機密性 3：極秘	● 法律で安全管理が義務付けられている ● 事業秘密として指定されている ● 漏えいすると会員大学，教員・学生に大きな影響がある
機密性 2：機構外秘	● 漏えいすると事業に大きな影響がある ● 守秘義務の対象として指定されている ● 限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている
機密性 1：公開	既に公知に公開しているもの

3.1.2. 情報資産の分類の表示

情報資産の機密性は以下の方法で表示する。

- 電子データ：保存先サーバのフォルダー名に表示
- 書類：保管先キャビネット，ファイル，バインダーに表示

表示が困難な場合は，「情報資産管理台帳」に機密性評価値を表示する。

3.1.3. 情報資産の管理責任者

情報資産の取り扱いに関する情報セキュリティの運用管理責任者は，当該情報資産を主に利用する部長とする。各種委員会が取り扱うものについては，その事務を担当している部の長が責任者となる。

3.1.4. 情報資産の利用者

情報資産の利用者の範囲は，「情報資産管理台帳」の利用者範囲欄に示された部門に従事する職員等及び機構委員とする。

3.2. 情報資産の機構外持ち出し

情報資産を機構外に持ち出す場合には，以下を実施する。

- 機密性２（機構外秘）の場合は所属部長の許可を得る
- 機密性３（極秘）の場合は理事長の許可を得る

3.2.1. 物理的に持ち出す場合には，以下を実施する。

- ノートパソコンのハードディスクに保存して持ち出す場合は，OS の機能を用いてデータを暗号化する。
- スマートフォン，タブレットに保存して持ち出す場合は，セキュリティロックを設定する。
- USB メモリ，HDD 等の電子媒体に保存して持ち出す場合は，ハードウェアロック機能を装備したものに限る。USB メモリ等の小型電子媒体は，大きなタグを付ける。

- 携行中は常に監視可能な距離を保つ。

3.2.2. クラウドストレージ等を用いて共有する場合には，以下を実施する。

- 機密性３（極秘）の情報を共有することは情報セキュリティ責任者の許可を得る。

3.3. 媒体の処分

3.3.1. 媒体の廃棄

機密性２(機構外秘)又は機密性３(極秘)の情報資産を廃棄する場合は以下の処分を行う。

書類・フィルム	細断/溶解/焼却
USB メモリ・HDD・CD・DVD	破壊/細断/完全消去 ※OS による削除・クイックフォーマットは不可

3.3.2. 媒体の廃棄は，情報システム管理室が担当する。

3.3.3. 媒体の再利用

機密性２(機構外秘)又は機密性３(極秘)の情報資産を保存した媒体を再利用する場合は，以下の処分を行う。

書類	裏紙再利用禁止
USB メモリ・HDD・CD-RW ディスク・DVD-RW ディスク	完全消去後再利用 ※OS による削除・クイックフォーマットは不可
CD-R・DVD-R	再利用不可

3.4. 情報資産およびそのバックアップの保管

3.4.1. 媒体としての保管

情報資産を機構内で保管する場合，鍵付のキャビネットあるいはサーバ室内にて保管する。

3.4.2. クラウドサービスを利用した保管

クラウドサービスを利用し，外部のサーバに情報を保存する場合は，以下のサービス要件を確認し，情報セキュリティ責任者の許可を得て導入する。

- サービス提供者のサービス利用約款，情報セキュリティ方針が，当機構の情報セキュリティ関連規程に適合している。
- 当機構あるいはクラウドサーバが立地する地域で発生する震災，水害等の影響を受けない地域の施設であること。

3.4.3. バックアップの取得

情報システム管理者は，情報データのバックアップを定期的に取得する。

4. アクセス制御及び認証（適用範囲：情報資産の利用者及び情報処理施設）

4.1. アクセス制御方針

機密性２（機構外秘）又は機密性３（極秘）の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

- 「情報資産管理台帳」の利用者範囲に基づき，利用者の業務・職務に応じた必要最低限のアクセス権を付与する。

4.2. 利用者の認証

機密性２（機構外秘）又は機密性３（極秘）の情報資産を扱う社内情報システムは，以下の方針に基づいて利用者の認証を行う。

- 利用者の認証に用いるアカウントは，利用者１名につき１つを発行する。
- 特に許可された場合を除き，同一アカウントの他者との共有および複数の利用者が共有するアカウントの発行を禁止する。

4.3. 利用者アカウントの登録

利用者の認証に用いるアカウントは，情報セキュリティ責任者の承認に基づき登録する。

4.4. 利用者アカウントの削除または無効化

利用者の認証に用いるアカウントが不要になる場合または利用者である職員が退職する場合，情報システム管理者は，原則として当該状況が発生する日の翌日までに，当該アカウントの削除又は無効化を実施し，情報セキュリティ責任者にその旨報告するものとする。

4.5. パスワードの設定

利用者の認証に用いるパスワードは，以下に注意して設定する。

- 十分な強度のあるパスワードを用いる
- 他者に知られないようにする

4.6. 職員等以外の者に対する利用者アカウントの発行

当機構の職員以外の者は，原則としてアカウントを発行しない。ただし，情報セキュリティ責任者が特に必要と認めた場合，秘密保持契約を締結した上で許可することがある。

5. 物理的対策（適用範囲：機構内）

5.1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル 1 領域	共有スペース
利用者	職員等，機構委員，外部関係者，部外者が立ち入り可
施錠	警備会社への通報装置作動
設置可能情報機器	無線 LAN 中継機器
制限事項	未使用時に機密性２（機構外秘）又は機密性３（極秘）の情報資産の放置禁止
部外者管理	建物管理会社の意向による

レベル 2 領域	機構執務室・役員室，会議室
利用者	職員等以外の入室は職員等の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	プロジェクター，ホワイトボード，パソコン，複合機，電話機 LAN ケーブルハブ，無線 LAN 中継器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	職員等の許可を受けて入室可能

レベル 3 領域	サーバールームおよび情報システム管理者が指定する場所
利用者	あらかじめ許可された者
施錠	常時施錠
設置可能情報機器	サーバ，ルータ等のネットワーク機器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止 スマートフォン，USB メモリ，HDD，CD-R，デジタルカメラその他の情報記憶媒体の無断持込み禁止
部外者管理	保守・点検時等に登録者のエスコート付で入室可能

5.2. セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

- 複合機，プリンタに原稿，印刷物を放置しない。
- FAX 送信時には誤送信防止のため宛先を複数回確認する。
- 外線受話時の際，既知の関係者以外に，職員の個人情報・所在等を伝えてはならない。

6. IT 機器利用（適用範囲：業務で利用する情報機器）

6.1. ソフトウェアの利用

6.1.1. 標準ソフトウェア

業務に利用するパソコンには，当機構の標準ソフトウェアを導入する。当機構の標準ソフトウェア以外のソフトウェアを導入する場合は，情報システム管理者の許可を得たうえで導入する。標準ソフトウェアは「6.6.1 標準ソフトウェア」を参照のこと。

6.1.2. ソフトウェアの利用制限

情報システム管理者は，利用者の業務に不要な機能をあらかじめ取除いて提供する。職員等および機構委員は，業務に不要なシステムユーティリティやソフトウェアを利用しない。

利用を禁止するソフトウェア

- インターネットを利用して，自動的に不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア
- 不審なベンダーが提供するソフトウェア
- 正規ライセンスを取得していないソフトウェア

6.1.3. ソフトウェアのアップデート

職員等は，業務で使用するソフトウェアを最新の状態で利用する。

6.1.4. ウイルス対策

6.1.4.1. ウイルス対策ソフト定義ファイルの更新

職員等は，パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。

6.1.4.2. 外部機器の LAN 接続

当機構が管理するパソコン及びサーバ以外の機器を機構内 LAN に接続することを禁止する。業務上必要な場合は，情報システム管理者に当該機器の MAC アドレスを届け出た上で接続の許可を取得するとともに，当該機器にインストールされているウイルス対策ソフトの定義ファイルを最新版に更新し，当該機器のフルスキャンを実行し，ウイルスが検知されないことを確認してから接続する

6.1.5. ウイルス対策の啓発

情報システム管理者は，適宜ウイルスに関する情報を収集し，重大な被害を与えるウイルスに対しては，対応策及び対応に必要な修正プログラムを社内に公開及び通知する。職員等は，感染防止策が通知された場合は，速やかに実施完了すること。

6.2. ＩＴ機器の利用

6.2.1. 職員等によるＩＴ機器の利用

職員等は，業務に利用するパソコン・タブレット・スマートフォンには，ログインパスワードを設定する。利用するときには以下を実行する。

- ログインパスワードを他者の目に触れる所に書き記さない。
- 屋外で利用する場合は，他者が画面を盗み見可能な環境で利用しない。

- 退社時又は使用しないときには電源を切り，ノートパソコン・タブレット・スマートフォン・USB メモリ，HDD，CD 等の電子媒体は施錠保管する。

6.2.2. 機構委員によるＩＴ機器の利用

機構委員が機構所有のＩＴ機器を利用する際には以下を実行する。

- 職員等から指示されたログイン ID，パスワードを使用する。
- 私有の USB メモリなどの記憶媒体の使用を禁止する。

6.3. クリアデスク・クリアスクリーン

6.3.1. クリアデスク

職員等は，機密性２（機構外秘）又は機密性３（極秘）の書類及び電子データを保存したノートパソコン，USB メモリ，HDD，CD 等の持ち運び可能な機器や媒体の扱いについて，以下のようにクリアデスクを徹底する。

- 利用時以外には机上に放置しない。
- 離席時に書類を伏せる，引き出しに入れる等する。
- 退社時又は使用しないときには机の引き出しに保管し，施錠する。

6.3.2. クリアスクリーン

職員等は，離席時に以下のいずれかによりパソコンの画面をロックし，クリアスクリーンを徹底する。

- ログオフ状態ではシステム操作画面は非表示に設定する。退社時又は使用しないときにはパソコンの電源を切る。
- スマートフォン・タブレットを外出先で利用する場合は，他者が盗み見できる環境で利用しない。

6.4. インターネットの利用

6.4.1. ウェブ閲覧

情報システム管理者は，ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイトはウェブフィルタリングソフトを使用して，職員等の閲覧を制限する。職員等は，業務でウェブ閲覧を行う場合は以下に注意する。

- 公序良俗に反するサイトへのアクセスを禁止する。
- 不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
- 業務上，個人情報(メールアドレス，氏名，所属等)を入力する場合は，通信の暗号化，接続先の実在性等を十分に確認したうえで行う。
- 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き，モバイルコード(クライアントパソコン側で動作するプログラム)を実行しない。

6.4.2. オンラインサービス

職員等は，インターネットで提供されているサービスを業務で利用する場合は，情報システム管理者の許可を得る。利用する際には以下に注意する。

インターネットバンキング・電子決済

- インターネットバンキングを利用する際には，自分で設定したブックマークや銀行が提

供する専用アプリケーションソフトを用いる。

- 電子決済を利用する際には，SSL/TLS による通信暗号化を採用しているサイトを利用する。
- 電子メールに記載されているリンクや，他のウェブサイト等に設置されているリンクは，偽サイトへの誘導である可能性があるためアクセスしない。

<u>オンラインストレージ</u>

- 機構が指定したオンラインストレージ以外を使用しない。機構が指定したオンラインストレージは「6.7.2 業務に使用するオンラインストレージ」を参照のこと。
- メールアドレスの登録が必要な場合は機構が提供するメールアドレスを登録する。

<u>e-learning システムおよび動画配信プラットフォーム</u>

- 機構が指定した e-learning システム及び動画配信プラットフォーム以外を使用しない。機構が指定した動画配信プラットフォームは，「6.7.3 業務に使用する e-learning および動画配信プラットフォーム」を参照のこと。

6.4.3. SNS の個人利用

- 機密性２（機構外秘）又は機密性３（極秘）の情報の書き込みは行わない。
- 取引先従業者あるいは機構委員と SNS 上で交流する場合，双方の立場をわきまえ，社会人として良識の範囲で交流する。
- SNS 用のアプリケーションが提供するセキュリティ設定を行い，アカウントの乗っ取りやなりすましに注意する。
- 使用するパソコン，スマートフォン，タブレット上のデータ，写真，位置情報が，予期せず公開される可能性のあることに注意する。

6.4.4. 電子メールの利用

職員等は，業務で電子メールを利用する際には以下を実施する。

<u>誤送信防止</u>

- 電子メールソフトの即時送信機能を停止する。

<u>メールアドレス漏えい防止</u>

- 同報メール（外部の多数相手に同時に送信するとき）を送信する場合は，宛先（TO）に自分自身のアドレスを入力し，BCC で複数相手のアドレスを指定する。

<u>傍受による漏えい防止</u>

- 機密性２（機構外秘）又は機密性３（極秘）の情報資産のメールによる送信は原則として行わない。業務上必要がある場合は，情報システム管理者の承認を得る。

<u>添付ファイル暗号化の方法</u>

- 添付ファイルを暗号化する場合，パスワードは先方とあらかじめ決めておくか，電話等で通知することとし，２通目のメールでパスワードを送信することを禁止する。

<u>禁止事項</u>

- 業務に支障をきたすおそれがある使用
- 私用電子メールサーバーへの接続

- 私用メールアドレスへの転送

6.4.5. ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため，以下の内容に複数合致する場合は十分に注意し，添付ファイルを開く，又はリンクを参照するなどしない。受信した場合は，情報システム管理者に報告し，情報システム管理者は社内に注意を促す。

メールのテーマ

- 知らない人からのメールだが，メール本文の URL や添付ファイルを開かないと内容が確認できない場合
- 心当たりのないメールだが，興味をそそられる内容
- これまで届いたことがない公的機関からのお知らせ
- 組織全体への案内
- 心当たりのない，決裁や配送通知（英文の場合が多い）
- ID やパスワードなどの入力を要求するメール

差出人のメールアドレス

- 登録のないフリーメールアドレスから送信されている
- 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる

メールの本文

- 日本語の言い回しが不自然である
- 実在する名称を一部に含む URL が記載されている
- 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる（HTML メールの場合）
- 署名の内容が誤っている（組織名や電話番号が存在しない，電話番号が FAX 番号として記載されている）

添付ファイル

- ファイルが添付されている
- 実行形式ファイル(exe/scr/cpl など)が添付されている
- ショートカットファイル(lnk など)が添付されている
- 二重拡張子となっている
- ファイル拡張子の前に大量の空白文字が挿入されている

6.5. ＩＴ機器の機構外への持ち出し

機構所有のＩＴ機器を持ち出して使用する場合は，以下を実施する。

- 情報セキュリティ部門管理者から，ＩＴ機器持ち出しの許可を得る。
- 持ち出す前に OS・ソフトウェアはインターネットに接続した状態で自動更新を有効にして最新の更新プログラムをインストールする。
- ウイルス対策ソフトの定義ファイルは自動で更新する。
- 社外でのソフトウェアインストールは禁止する。
- インターネット接続時には機構が貸与するモバイル Wi-Fi ルータを使用することとし，

自宅の回線，公衆 Wi-Fi サービスなどの利用は禁止する。

6.6. 私有ＩＴ機器・電子媒体の利用

6.6.1. 利用の可否

6.6.1.1. 職員等の私有ＩＴ機器・電子媒体

職員等が所有するパソコン，タブレット，スマートフォン，携帯電話等のＩＴ機器及び USB メモリ，HDD，CD 等の電子媒体を業務で利用することは禁止する。

6.6.1.2. 機構委員の私有ＩＴ機器・電子媒体

6.6.1.2.1. 機構委員が所有するパソコン，タブレット，スマートフォン，携帯電話等のＩＴ機器及を機構内に保ちこんで使用する際には，原則として機構のネットワークへの接続を禁止する。ただし，情報システム管理者が必要と認めた場合はその限りではない。

6.6.1.2.2. 機構委員が所有する USB メモリ，HDD，CD 等の電子媒体（所属大学が所有するものを含む）を機構内ネットワークに接続された端末で使用することは禁止する。

6.6.1.3. 機構委員の私有ＩＴ機器の端末認証

機構ネットワークに接続する私有ＩＴ機器・電子媒体は，ネットワークアドレス（ＭＡＣアドレス）を用いた端末認証を行う。

6.6.2. 私有ＩＴ機器の利用開始時

6.6.2.1. 機構委員が私有 IT 機器を機構内に持ち込んで使用する際には以下を実行する。

- ウイルス対策ソフトウェアをインストールし，定義ファイルを更新する。
- ハードディスク，電子媒体に対してウイルスチェックを行う。

6.6.2.2. 情報システム管理者が機構委員私有 IT 機器の機構ネットワークへの接続を認めた場合，利用を開始する前に利用する本人が以下を実行する。

- 接続する私有ＩＴ機器のネットワークアドレス（ＭＡＣアドレス）を情報システム管理者に届け出て，利用の許可を得る。
- 情報システム管理者が承認したウイルス対策ソフトウェアをインストールし，定義ファイルを更新する。
- ハードディスク，電子媒体に対してウイルスチェックを行う。
- ゲスト用として準備された Wi-Fi アクセスポイント以外への接続は禁止する。

6.6.3. 私有ＩＴ機器の利用期間中

利用期間中は，以下の各項目を遵守する。

- ウイルス対策ソフトウェアの定義ファイルを常に最新の状態に保つ
- OS やアプリケーションソフトのアップデートを速やかに行う。
- 機構内で利用したデータを個人のアドレスに送信しない。
- 機密性２（機構外秘）又は機密性３（極秘）の情報資産を保存しない。
- 以下のアプリケーションソフトのインストールおよび利用をしない。
  - 機器ベンダーの公式な公開場所（App Store，Google Play など）以外から提供されるもの
  - 正規ライセンスを取得していない違法なもの

6.7. 標準ソフトウェア等

6.7.1. 標準ソフトウェア

種別	名称	開発・販売元	バージョン
パソコン OS	Windows Mac OS	Microsoft Apple	Windows10 以降 Mac OS 13 以降
オフィス系ソフト	Office	Microsoft	Office365

6.7.2. 業務に使用するオンラインストレージ

- DirectCloud
- Microsoft OneDrive, Sharepoint, Teams
- Box

6.7.3. 業務に使用する e-learning および動画配信プラットフォーム

- CLEVAS
- Learning Ware
- ナレッジデリ

7. IT 基盤運用管理（適用範囲：サーバ，ネットワーク及び周辺機器）

7.1. 管理体制

情報システム管理者は，ＩＴ基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は，情報セキュリティ責任者が承認する。

7.2. ＩＴ基盤の情報セキュリティ対策

7.2.1. サーバ機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバ機器に求める情報セキュリティ要件は，情報システム管理者が決定する。新規にサーバ機器を導入する場合は，情報セキュリティ要件を満たす製品を選択し，情報システム管理者の許可を得て導入する。

7.2.2. ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器に求める情報セキュリティ要件は，情報システム管理者が決定する。新規にネットワーク機器を導入する場合は，情報セキュリティ要件を満たす製品を選択し，情報システム管理者の許可を得て導入する。

7.3. ＩＴ基盤の運用

情報システム管理者は，ＩＴ基盤の運用を行う際には以下を実施すること。

- 情報システム管理者は，機器の管理画面にログインするためのパスワードは初期状態のまま使わず，推測不可能なパスワードを設定して運用する。
- 以下に従い，ゲートウェイにおける通信ログを取得及び保存する。
  - 通信ログの保存期間は 3 年間とする。
  - ログファイルの保存状況について，情報システム管理者が定期的に確認する。
- 情報システム管理者は，通信ログについて以下の確認を定期的に行う。
  - 管理外のインターネット接続がないか
  - 許可なく接続された機器や無線 LAN 機器はないか
  - 不審な通信が行われていないか
- 情報システム管理者は，必要に応じて業務に不要なウェブサイト閲覧を職員への周知により制限する。
- 遠隔診断ポートの利用は，保守サポートなど必要な場合のみに限定し，認証機能やコールバック機能等を備えるなど，適切なセキュリティ対策を施す。

7.4. クラウドサービスの導入

ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は，情報システム管理者がサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。新規クラウドサービス等の外部サービスを導入する場合は，情報システム管理者の許可を得て導入する。サービスプロバイダの情報セキュリティ対策の評価基準は，「7.2 クラウドサービスの情報セキュリティ要件」を参照のこと。

7.5. 脅威や攻撃に関する情報の収集

情報システム管理者は，最新の脅威や攻撃に関する情報収集を行い，必要に応じて機構内で共有する。

7.6. 廃棄・返却・譲渡

情報システム管理者は，ＩＴ基盤で利用した機器を返却，廃棄，譲渡を行う場合は，内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し，情報セキュリティ責任者の承認を得たうえ返却，廃棄，譲渡を行う。内部記憶媒体の破壊又はデータの完全消去を，外部に委託する場合は，破壊又はデータの完全消去を実行したことの証明書を取得する。

7.7. ＩＴ基盤の情報セキュリティ要件及び標準

7.7.1. 機器・ソフトウェアの情報セキュリティ要件及び標準

ＩＴ基盤で利用する機器及びソフトウェアの情報セキュリティ要件と，それに基づく機構標準を以下とする。

ファイルサーバ

- 利用者認証機能を有する。
- セキュリティログ取得機能を有する。
- システムログ取得機能を有する。
- ユーザーアクセスログ取得機能を有する。

ネットワーク機器の情報セキュリティ要件

- 利用者認証機能を有する。
- MAC アドレス認証機能を有する。
- 通信ログ取得を有する。
- ユーザーアクセス監視を有する。

7.7.2. クラウドサービスの情報セキュリティ要件

ＩＴ基盤で利用するクラウドサービスの情報セキュリティ要件を以下とする

- サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が，処理しようとする情報資産の重要度に照らして適切であること。
- サービス仕様に含まれる情報セキュリティ対策が，処理しようとする情報資産の重要度に照らして適切であること。
- 情報セキュリティに関する適合性評価制度の認証・認定を取得していること。

※ 参考　適合制評価制度の種類

- 情報セキュリティマネジメントシステム適合性評価制度(ISMS クラウドセキュリティ認証)
- クラウド情報セキュリティ監査制度
- プライバシーマーク制度
- クラウドサービスの安全・信頼性に係る情報開示認定制度
- ISMAP 政府情報システムのためのセキュリティ評価制度

8. システム開発及び保守（適用範囲：機構が独自に開発する情報システム）

8.1. 新規システム開発・改修

情報システムの開発・改修を行う際には，以下の工程を経て実施する。各工程の完了時に情報システム管理者の承認を得る。

① 対象業務の範囲定義
② ハードウェア・ソフトウェア・ネットワーク機能検討
③ 必要なパフォーマンスの検討
④ 情報セキュリティ要件定義
⑤ バックアップ/障害復旧要件定義
⑥ 情報システム運用要件定義
⑦ 運用体制
⑧ 移行計画立案

8.2. 脆弱性への対処

情報システムのソフトウェア開発を行う際には，当該情報システムの利用環境に応じて設計時に技術的な脆弱性を識別し，対策を講じる。脆弱性に対する対策の有効性は情報システム管理者が判断し，承認する。

8.3. 情報システムの開発環境

情報システムの開発及び改修を行う環境は，運用環境とは分離する。新たに情報システムの開発を行った場合や，情報システムの改修を行った場合は，当該情報システムの運用を開始する前に，必要な情報セキュリティ対策が講じられていることを確認し，情報システム管理者の承認を得る。

8.4. 情報システムの保守

情報システムの保守は，開発元又は外部の組織に委託することを原則とするが，それができない場合，以下に挙げる事項に留意し，情報システムに既知の脆弱性が存在しない状態で運用する。

- 開発時に用いたソフトウェアに関する脆弱性が公表された場合には，速やかにその影響が顕在化しないための対策を講じる。
- 開発時に用いたソフトウェア及びハードウェアの製造者が提供するサポートの終了が予定されている場合，他のソフトウェアやハードウェアを用いた再構築又は当該情報システムの利用停止を検討し，情報システム管理者の承認を得る。

8.5. 情報システムの変更

情報システムのハードウェア又はソフトウェアの変更を行う際には，以下の工程を経て実施する。各工程の完了時に情報システム管理者の承認を得る。

- 現行システムの問題・課題の把握
- システム変更計画立案
- システム変更計画書に基づくシステム設計

- セキュリティ要求と設計の見直し
- 移行計画立案（移行時，運用時の障害対応をあらかじめ検討する。）
- 変更後の仕様書，操作手順書，運用手順書等の関連文書の作成

9. 委託管理（適用範囲：情報資産を取り扱う業務の委託）

9.1. 委託先評価基準

情報セキュリティ部門責任者は情報資産を取り扱う業務を，外部の組織に委託する場合は，委託先の情報セキュリティ管理について，以下の基準に基づいて評価する。

- 情報セキュリティマネジメントシステム（ISMS）適合性評価制度の認証を取得している。
- 個人情報保護マネジメントシステム（PMS）に適合し，プライバシーマーク付与を受けている。
- 情報セキュリティ監査を定期的に実施している。
- 情報セキュリティに関する方針を公開している。

9.2. 委託先の選定

評価結果に基づき委託先を選定し，情報セキュリティ責任者の承認を得る。

9.3. 委託契約の締結

委託契約書には，下記に関する事項を明記する。

- 当機構の情報資産及び個人情報の守秘義務
- 再委託についての事項
- 事故時の責任分担についての事項
- 委託業務終了時の当社が提供した情報資産及び個人情報の返却又は廃棄，消去についての事項
- 情報セキュリティ対策の実施状況に関する監査の方法とその権限
- 契約内容が遵守されない場合の措置
- 事故発生時の報告方法

9.4. 再委託

機構が委託する業務を，委託先が他の組織又は個人に再委託する場合には，事前に書面による報告を委託先に求める。報告には必要に応じて以下の提供を含め，当機構の「1.委託先評価基準」「3.委託契約の締結」「4.委託先の評価」と同等の管理を再委託先に求めていることを確認し，情報セキュリティ責任者の承認を得たうえで再委託を認める。

- 委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
- 再委託先の選定基準
- 再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその証書の写し

10. 情報セキュリティインシデント対応

10.1. 対応体制

情報セキュリティインシデントが発生した場合には，以下の体制で対応する。

最高責任者	理事長
対応責任者	部門責任者
一次対応者	発見者又は情報システム管理者

10.2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合,以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	責任者
3	●会員大学，教員・学生等に影響が及ぶとき ●個人情報が漏えいしたとき	理事長
2	事業に影響が及ぶとき	インシデント対応責任者
1	従業員の業務遂行に影響が及ぶとき	インシデント対応責任者
0	インシデントにまでは至らないが，将来においてインシデントが発生する可能性がある事象が発見されたとき	情報システム管理者

10.3. インシデントの連絡及び報告

事故レベル 1 以上のインシデントが発生した場合，発見者は予め決められた連絡網に従い，対応者または責任者に速やかに報告し，指示を仰ぐ。

10.4. 対応手順

インシデントを以下のとおりに区分し，それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	機密性２（機構外秘）又は機密性３（極秘）情報資産の盗難，流出，紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん，消失，破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

10.4.1. 漏えい・流出発生時の対応

事故レベル３

① 発見者は即座にインシデント対応責任者及び理事長に報告する。

② インシデント対応責任者は原因を特定するとともに，二次被害が想定される場合には防止策を実行する。

③ インシデント対応責任者は被害者/本人対応を準備する。

④ インシデント対応責任者は問い合わせ対応を準備する。

⑤ インシデント対応責任者は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請する。

⑥ インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。

⑦ インシデント対応責任者は個人データまたは特定個人情報漏えいの場合には理事会に報告する。

⑧ 理事長は機構内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

事故レベル２

① 発見者は発見次第，情報システム管理者に報告する。

② 情報システム管理者は漏えい先を調査し，インシデント対応責任者に報告する。

③ 情報システム管理者は社内関係者に周知する。

事故レベル１

※ 情報漏えい・流出は全て事故レベル 2 以上

10.4.2. 改ざん・消失・破壊・サービス停止発生時の対応

事故レベル３

① 発見者は即座にインシデント対応責任者及び理事長に報告する。

② 情報システム管理者は原因を特定し，応急処置を実行する。

③ インシデント対応責任者は機構に周知する。

④ 電子データの場合は情報システム管理者がバックアップによる復旧を実行する。

⑤ 機器の場合は情報システム管理者が修理，復旧，交換等の手続きを行う。

⑥ 書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

⑦ 情報システム管理者は原因対策を実施する。

⑧ 理事長は機構内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

事故レベル２

① 発見者は発見次第，情報システム管理者に報告する。

② 情報システム管理者は原因を特定し，応急処置を実行する。

③ インシデント対応責任者は社内に周知する。

④ 電子データの場合は情報システム管理者がバックアップによる復旧を実行する。

⑤ 機器の場合は情報システム管理者が修理，復旧，交換等の手続きを行う。

⑥ 書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

⑦ 情報システム管理者は原因対策を実施する。

事故レベル１

① 発見者は発見次第，情報システム管理者に報告する。

② 情報システム管理者は原因を特定し，応急処置を実行するとともに必要に応じて機構内に周知する。

③ 電子データの場合は情報システム管理者がバックアップによる復旧又は再作成・入手を実行する。

④ 機器の場合は情報システム管理者が修理，復旧，交換等の手続きを行う。

⑤ 書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

⑥ 情報システム管理者は原因対策を実施する。

事故レベル０

発見者は発見次第，発生可能性のあるインシデントと想定される被害を情報システム管理者に報告する。

10.4.3. ウイルス感染時の初期対応

職員等は，業務に利用しているパソコン，サーバー又はスマートフォン，タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には，以下を実行する。

① ネットワークからコンピュータを切断する。

② 情報システム管理者に連絡する。

③ ウイルス対策ソフトの定義ファイルが最新の状態でない場合は最新版に更新する。

※他のコンピュータでネットワークに接続し，定義ファイルの最新版をダウンロードしたうえで，感染したコンピュータの定義ファイルを更新する。

④ ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥ 駆除後再度ウイルス対策ソフトでスキャンし，駆除を確認する。

⑦ 情報システム管理者に報告する。

⑧ 従業員自身で対応できないと判断される場合は情報システム管理者に問い合わせる。

10.5. 届出及び相談

情報システム管理者は，インシデント対応後に以下の機関への届け出，報告又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター】

https://www.ipa.go.jp/security/todokede/crack-virus/about.html